

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 15 of 25

Remarks

The present amendment replies to a Final Office Action dated February 17, 2006. Claims 1, 2, and 4-39 are currently pending in the present application. Claims 1, 4, 6, 10, 13, 16, 25, 27, and 29 have been amended and claim 40 added herein. In the Final Office Action, the Examiner rejected pending claims 1, 2, and 4-39 on various grounds. The Applicants respond to each ground of rejection as subsequently recited herein and respectfully request reconsideration and further examination of the present application.

The Applicants wish to thank Examiner Pich for his interview with the Applicants' attorney on March 21, 2006, and Interview Summary dated April 10, 2006, which completely and accurately records the substance of the interview.

- A. Claims 10-39 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

The paragraph starting on page 16, line 19, of the specification has been amended to further clarify that the client public key is stored exclusively outside the client. The paragraph starting on page 25, line 17, and ending on page 26, line 4, which included an alternative embodiment with the client transmitting the client public key in a client request message, has been deleted herein. No new matter has been added with these amendments. Withdrawal of the rejection of claims 10-39 under 35 U.S.C. §112, first paragraph, is respectfully requested.

- B. Claims 1-2 and 4-5 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

Claim 1 has been amended to delete the reference to the serial number, which has been included in new dependent claim 40. Claims 2 and 4-5 depend on independent claim 1 and

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 16 of 25

include all the elements and limitations of independent claim 1. Withdrawal of the rejection of claims 1-2 and 4-5 under 35 U.S.C. §112, second paragraph, is respectfully requested.

C. Claims 6-8 were rejected under 35 U.S.C. §102(b), as being anticipated by U.S. Patent No. 5,559,889 to *Easter, et al.*

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the . . . claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The Applicants have thoroughly considered the Examiner's remarks concerning patentability of claims 6-8 over U.S. Patent No. 5,559,889 to *Easter, et al.* (the "*Easter* patent"). The Applicants have also thoroughly read the *Easter* patent. The Applicants traverse this rejection and assert that the *Easter* patent fails to disclose, teach, or suggest an article of manufacture including a first read-only memory structure containing an embedded private cryptographic key, the embedded private cryptographic key being associated with a stored public cryptographic key stored exclusively outside the first read-only memory structure; and a second read-only memory structure containing an embedded public cryptographic key, wherein the embedded public cryptographic key and the embedded private cryptographic key are not related by a cryptographic public/private key pair relationship, as recited in independent claim 6.

The *Easter* patent discloses designating a private key/public key pair for the IC chip. Fuse array 51 is encoded with the private key. Further, the fuse array is encoded with the hash value for the corresponding public key and a serial number. See column 5, lines 39-44. The *Easter* patent fails to disclose a second read-only memory structure containing an embedded public cryptographic key, as recited in amended independent claim 6. The *Easter* patent fails

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 17 of 25

to disclose the embedded private cryptographic key being associated with a stored public cryptographic key stored exclusively outside the first read-only memory structure, as recited in amended independent claim 6.

Claims 7 and 8 depend directly or indirectly from amended independent claim 6. Therefore, dependent claims 7 and 8 include all the elements and limitations of their respective independent claims. The Applicants respectfully submit that dependent claims 7 and 8 are allowable over the *Easter* patent for at least the same reason as set forth above with respect to their respective independent claims.

Withdrawal of the rejection of claims 6-8 under 35 U.S.C. §102(b) as being anticipated by the *Easter* patent is respectfully requested.

- D. Claim 9 was rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,559,889 to *Easter, et al.* in view of ecommerce-guide.com ("A Framework For SmartCard Payment Systems - Part One" by Mark Merkow, June 22, 2000).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references when combined must teach or suggest all the claim limitations. *See* MPEP 2143. This rejection is traversed.

Claim 9 was rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,559,889 to *Easter et al.* (the "*Easter* patent") in view of ecommerce-guide.com ("A Framework For SmartCard Payment Systems - Part One" by Mark Merkow, June 22, 2000) (the "*Merkow* article"). The Applicants have thoroughly considered the Examiner's remarks concerning patentability of claim 9 over the *Easter* patent in view of the *Merkow* article. The Applicants have also thoroughly read the *Easter* patent and the *Merkow* article. As discussed in

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 18 of 25

Section C above, the Applicants assert that the *Easter* patent fails to disclose, teach, or suggest an article of manufacture including a second read-only memory structure containing an embedded public cryptographic key, as recited in independent claim 6. The *Merkow* article also fails to disclose, teach, or suggest the same. Claim 9 depends indirectly from independent claim 6 and so includes all the elements and limitations of the respective independent claim 6 and intervening claims 7 and 8. The Applicants respectfully submit that dependent claim 9 is allowable over the *Easter* patent and the *Merkow* article for at least the same reasons as set forth above with respect to independent claim 6 and dependent claims 7 and 8.

Withdrawal of the rejection of claim 9 under 35 U.S.C. §103(a), as being unpatentable over the *Easter* patent in view of the *Merkow* article is respectfully requested.

E. Claims 1, 2, 4-5, 10, 13, 16, 19, 21, 23, 31, 34, 37, 32, 35, 38, 33, 36, and 39, were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold* in view of U.S. Patent No. 5,970,147 to *Davis*.

The Applicants have thoroughly considered the Examiner's remarks concerning patentability of claims 1, 2, 4-5, 10, 13, 16, 19, 21, 23, 31, 34, 37, 32, 35, 38, 33, 36, and 39 over U.S. Patent No. 5,787,172 to *Arnold* (the "*Arnold* patent") in view of U.S. Patent No. 5,970,147 to *Davis* ("*Davis* patent"). The Applicants have also thoroughly read the *Arnold* and *Davis* patents. The Applicants traverse this rejection and assert that the *Arnold* and *Davis* patents, alone or in combination, fail to disclose, teach, or suggest:

a method for configuring a semiconductor chip including selecting a public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic public/private key pair relationship; and storing a second public cryptographic key associated with the private cryptographic key exclusively outside the semiconductor chip, as recited in amended independent claim 1;

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 19 of 25

a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship, the embedded client private key being associated with a client public key stored exclusively outside the client; means for the same; and instructions for the same, as recited in amended independent claims 10, 13, or 16, respectively;

a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client; means for the same; and instructions for the same, as recited in independent claims 19, 21, or 23, respectively; or

a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key stored exclusively outside the client; means for the same; and instructions for the same, as recited in independent claims 31, 34, or 37, respectively.

The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 20 of 25

MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit. See column 4, lines 11-27. The *Arnold* patent fails to disclose storing a second public cryptographic key associated with the private cryptographic key exclusively outside the semiconductor chip, as recited in amended independent claim 1; the embedded client private key being associated with a client public key stored exclusively outside the client, as recited in amended independent claims 10, 13, or 16; the client public key being stored exclusively outside the client, as recited in independent claims 19, 21, or 23; or the embedded client private key being associated with a client public key stored exclusively outside the client, as recited in independent claims 31, 34, or 37. The *Davis* patent also fails to disclose this element.

Claims 2 and 4-5; claims 32 and 33; claims 35 and 36; and claims 38 and 39 depend directly or indirectly from independent claims 1, 31, 34, and 37, respectively, and include all the elements and limitations of their respective amended independent claims. As discussed above, the *Arnold* and *Davis* patents, alone or in combination, fail to disclose a client private key associated with a client public key stored exclusively outside the client. Therefore, the *Arnold* and *Davis* patents fail to disclose all the limitations of the rejected claims. The Applicants respectfully submit that Claims 2, 4-5, 32, 33, 35, 36, 38, and 39 are allowable for at least the reasons discussed above for their respective amended independent claims.

Withdrawal of the rejection of claims 1, 2, 4-5, 10, 13, 16, 19, 21, 23, 31, 34, 37, 32, 35, 38, 33, 36, and 39 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Davis* patent is respectfully requested.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 21 of 25

F. Claims 11, 14, 17, 12, 15, 18, 20, 22, and 24 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold* in view of U.S. Patent No. 5,970,147 to *Davis* and further in view of U.S. Patent Publication No. US 2002/0078344 to *Sandhu, et al.*

As discussed in Section E above, the *Arnold* patent fails to disclose, teach, or suggest the embedded client private key being associated with a client public key stored exclusively outside the client, as recited in amended independent claims 10, 13, or 16; the client public key being stored exclusively outside the client, as recited in independent claims 19, 21, or 23; or the embedded client private key being associated with a client public key stored exclusively outside the client, as recited in independent claims 31, 34, or 37. The *Davis* patent also fails to disclose this element, as does U.S. Patent Publication No. US 2002/0078344 to *Sandhu, et al.* ("*Sandhu* publication"). Therefore, Applicants traverse this rejection.

Claims 11 and 12; claims 14 and 15; claims 17 and 18; claim 20; claim 22; and claim 24 depend directly or indirectly from independent claims 10, 13, 16, 19, 21, and 23, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Davis* patents and the *Sandhu* publication, alone or in combination, fail to disclose a client private key associated with a client public key stored exclusively outside the client. Therefore, the *Arnold* and *Davis* patents and the *Sandhu* publication fail to disclose all the limitations of the rejected claims. The Applicants respectfully submit that claims 11, 14, 17, 12, 15, 18, 20, 22, and 24 are allowable for at least the reasons discussed above for their respective amended independent claims.

Withdrawal of the rejection of claims 11, 14, 17, 12, 15, 18, 20, 22, and 24 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Davis* patent and further in view of the *Sandhu* publication is respectfully requested.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 22 of 25

- G. Claims 25, 27, and 29 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold* in view of U.S. Patent No. 5,559,889 to *Easter, et al.* and further in view of U.S. Patent No. 5,970,147 to *Davis*.

The Applicants traverse this rejection and assert that the *Arnold, Easter, and Davis* patents, alone or in combination, fail to disclose, teach, or suggest:

a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client; wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship; means for the same; and instructions for the same, as recited in independent claims 25, 27, and 29, respectively.

The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit. See column 4, lines 11-27. The *Arnold* patent fails to disclose the client public key corresponds to an embedded client private key in a read-only memory structure in

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 23 of 25

an article of manufacture in the client and is stored exclusively outside the client, as recited in independent claims 25, 27, and 29. The *Easter* and *Davis* patents also fail to disclose this element.

Withdrawal of the rejection of claims 25, 27, and 29 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Easter* patent and further in view of the *Davis* patent is respectfully requested.

H. Claims 26, 28, and 30 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold* in view of U.S. Patent No. 5,559,889 to *Easter, et al.* and further in view of U.S. Patent No. 5,970,147 to *Davis*, and further in view of U.S. Patent Publication No. US 2002/0078344 to *Sandhu, et al.*

As discussed in Section G above, the *Arnold* patent fails to disclose, teach, or suggest the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client, as recited in independent claims 25, 27, and 29. The *Easter* and *Davis* patents and *Sandhu* publication also fail to disclose this element. Therefore, Applicants traverse this rejection.

Claims 26, 28, and 30 depend directly from independent claims 25, 27, and 29, respectively, and include all the elements and limitations of their respective independent claims. Therefore, the *Arnold*, *Easter*, and *Davis* patents and the *Sandhu* publication fail to disclose all the limitations of the rejected claims. The Applicants respectfully submit that claims 26, 28, and 30 are allowable for at least the reasons discussed above for their respective independent claims.

Withdrawal of the rejection of claims 26, 28, and 30 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Easter* patent and further in view of the *Davis* patent and further in view of the *Sandhu* publication is respectfully requested.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 24 of 25

I. Claim 40 has been added herein.

Claim 40 has been added to incorporate the elements of claim 3, now cancelled. No new matter has been added with the addition of claim 40. Claim 40 is allowable over the cited references for at least the reasons discussed above for the respective independent claim 1.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 25 of 25


Summary

Reconsideration of claims 1, 2, and 4-39 as amended and consideration of claim 40 is respectfully requested in light of the remarks herein. The Applicants submit that claims 1, 2, and 4-40 as set forth by this Amendment fully satisfy the requirements of 35 U.S.C. §§ 102, 103, and 112. In view of foregoing remarks, favorable consideration and early passage to issue of the present application are respectfully requested.

Dated: May 15, 2006

Respectfully submitted,
David J. Craft, et al

CARDINAL LAW GROUP
1603 Orrington Avenue, Suite 2000
Evanston, IL 60201
(847) 905-7111


Frank C. Nicholas
Registration No. (33,983)
Attorney for Applicants